Konfigurieren und Registrieren eines Cisco IOS-Routers für einen anderen als CA-Server konfigurierten Cisco IOS-Router

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Cisco IOS®-Router als CA-Server (Certificate Authority) konfigurieren. Außerdem wird veranschaulicht, wie ein anderer Cisco IOS-Router registriert wird, um ein Root- und ID-Zertifikat für die IPsec-Authentifizierung vom CA-Server zu erhalten.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Zwei Cisco Router der Serie 2600 mit Cisco IOS Software, Version 12.3(4)T3.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Generieren und Exportieren des RSA-Schlüsselpaars für den Zertifikatsserver

Der erste Schritt besteht darin, das RSA-Schlüsselpaar zu generieren, das der Cisco IOS CA-Server verwendet. Generieren Sie auf dem Router (R1) die RSA-Schlüssel, wie folgende Ausgabe zeigt:

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable
The name for the keys will be: cisco1
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

R1(config)#
*Jan 22 09:51:46.116: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Hinweis: Sie müssen den gleichen Namen für das Schlüsselpaar (*Schlüsselbezeichnung*) verwenden, den Sie für den Zertifikatsserver verwenden möchten (über den **später beschriebenen Befehl crypto pki server *cs-label***).

Exportieren des generierten Schlüsselpaars

Exportieren Sie die Schlüssel in einen nichtflüchtigen RAM (NVRAM) oder TFTP (je nach

Konfiguration). In diesem Beispiel wird NVRAM verwendet. Abhängig von Ihrer Implementierung können Sie zum Speichern Ihrer Zertifikatsinformationen einen separaten TFTP-Server verwenden.

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123

% Key name: cisco1
   Usage: General Purpose Key
Exporting public key...
Destination filename [cisco1.pub]?
Writing file to nvram:cisco1.pub
Exporting private key...
Destination filename [cisco1.prv]?
Writing file to nvram:cisco1.prv
R1(config)#
```

Wenn Sie einen TFTP-Server verwenden, können Sie das generierte Schlüsselpaar erneut importieren, wie der folgende Befehl zeigt:

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable] passphrase
```

Hinweis: Wenn der Schlüssel nicht vom Zertifikatsserver exportiert werden soll, importieren Sie ihn zurück zum Zertifikatsserver, nachdem er als nicht exportierbares Schlüsselpaar exportiert wurde. Auf diese Weise kann der Schlüssel nicht wieder abgenommen werden.

Überprüfen Sie das generierte Schlüsselpaar.

Geben Sie den Befehl **show crypto key mypubkey rsa** ein, um das generierte Schlüsselpaar zu überprüfen.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 09:51:45 UTC Jan 22 2004
Key name: cisco1
 Usage: General Purpose Key
 Key is exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00CC2DC8 ED26163A
  B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83 F7B2BD56 126E0F11 50552843
  7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001
% Key pair was generated at: 09:51:54 UTC Jan 22 2004
Key name: cisco1.server
 Usage: Encryption Key
 Key is exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578 025D3066
  72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698
  EBD02905 FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1
  C1607433 5C7BC549 D532D18C DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

Aktivieren des HTTP-Servers auf dem Router

Der Cisco IOS CA-Server unterstützt nur Registrierungen, die über das Simple Certificate Enrollment Protocol (SCEP) erfolgen. Daher muss der Router den integrierten Cisco IOS HTTP-Server ausführen, um dies zu ermöglichen. Verwenden Sie den Befehl **ip http server**, um ihn zu aktivieren:

```
R1(config)#ip http server
```

Aktivieren und Konfigurieren des CA-Servers auf dem Router

Gehen Sie wie folgt vor:

1. Beachten Sie, dass der Zertifikatsserver den gleichen Namen wie das Schlüsselpaar verwenden muss, das Sie gerade manuell erstellt haben.Die Bezeichnung entspricht dem generierten Schlüsselpaarlabel:
   ```
   R1(config)#crypto pki server cisco1
   ```

   Nachdem Sie einen Zertifikatsserver aktiviert haben, können Sie die vorkonfigurierten Standardwerte verwenden oder Werte über CLI für die Funktionalität des Zertifikatsservers angeben.
2. Der **Datenbank-URL-**Befehl gibt den Speicherort an, an dem alle Datenbankeinträge für den CA-Server geschrieben werden. Wenn dieser Befehl nicht angegeben ist, werden alle Datenbankeinträge in Flash geschrieben.
   ```
   R1(cs-server)#database url nvram:
   ```

   Hinweis: Wenn Sie einen TFTP-Server verwenden, muss die URL **tftp://<ip_address>/directory** lauten.
3. Konfigurieren Sie die Datenbankebene:
   ```
   R1(cs-server)#database level minimum
   ```

   Mit diesem Befehl wird festgelegt, welche Datentypen in der Datenbank für die Zertifikatsregistrierung gespeichert werden:**Minimum** - Es werden genügend Informationen gespeichert, um weiterhin neue Zertifikate ohne Konflikte auszustellen. Der Standardwert.**Namen**: Zusätzlich zu den Informationen, die in der Mindeststufe angegeben sind, müssen die Seriennummer und der Betreffname jedes Zertifikats angegeben werden.**Complete (Abgeschlossen)**: Zusätzlich zu den Informationen, die in der Minimal- und der Namensebene angegeben sind, wird jedes ausgestellte Zertifikat in die Datenbank geschrieben.**Hinweis:** Das **vollständige** Schlüsselwort erzeugt eine große Menge an Informationen. Wenn sie ausgegeben wird, sollten Sie auch einen externen TFTP-Server angeben, auf dem die Daten über den **Datenbank-URL-**Befehl gespeichert werden sollen.
4. Konfigurieren Sie den Namen des CA-Emittenten in die angegebene DN-Zeichenfolge. In diesem Beispiel werden die CN (Common Name) von cisco1.cisco.com, L (Locality) von RTP und C (Country) von US verwendet:
   ```
   R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
   ```

5. Geben Sie die Lebensdauer (in Tagen) eines Zertifizierungsstellenzertifikats oder Zertifikats an.Gültige Werte liegen zwischen *1 Tag und 1825 Tagen*. Die standardmäßige Lebensdauer eines Zertifizierungsstellenzertifikats beträgt drei Jahre, und die standardmäßige Lebensdauer eines Zertifikats beträgt ein Jahr. Die maximale Lebensdauer eines Zertifikats

beträgt *einen Monat weniger* als die Lebensdauer des Zertifikats der Zertifizierungsstelle. Beispiel:

```
R1(cs-server)#lifetime ca-certificate 365
R1(cs-server)#lifetime certificate 200
```

6. Definieren Sie die Lebensdauer des vom Zertifikatsserver verwendeten CRL in Stunden. Der maximale Lebenszeitwert beträgt **336 Stunden** (zwei Wochen). Der Standardwert ist **168 Stunden** (eine Woche).

```
R1(cs-server)#lifetime crl 24
```

7. Definieren Sie einen CDP (Certificate Revocation List Distribution Point), der in den Zertifikaten verwendet werden soll, die vom Zertifikatsserver ausgegeben werden.Beim URL muss es sich um eine HTTP-URL handeln. Beispielsweise hatte unser Server die IP-Adresse 172.18.108.26:

```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. Führen Sie den Befehl **no shutdown aus**, um den CA-Server zu aktivieren:

```
R1(cs-server)#no shutdown
```

Hinweis: Geben Sie diesen Befehl nur dann aus, wenn Sie den Zertifikatsserver vollständig konfiguriert haben.

Konfigurieren und Registrieren des zweiten IOS-Routers (R2) für den Zertifikatsserver

Befolgen Sie dieses Verfahren.

1. Konfigurieren Sie einen Hostnamen und einen Domänennamen, und generieren Sie die RSA-Schlüssel auf R2.Verwenden Sie den Befehl **hostname**, um den Hostnamen des Routers als R2 zu konfigurieren:

```
Router(config)#hostname R2
R2(config)#
```

Beachten Sie, dass sich der Hostname des Routers unmittelbar nach Eingabe des Befehls **hostname** geändert hat.Verwenden Sie den Befehl **ip domain-name**, um den Domänennamen auf dem Router zu konfigurieren:

```
R2(config)#ip domain-name cisco.com
```

Verwenden Sie den Befehl **crypto key generate rsa**, um das R2-Schlüsselpaar zu generieren:

```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
```

2. Verwenden Sie diese Befehle im globalen Konfigurationsmodus, um gegenüber der CA zu deklarieren, dass der Router verwendet werden soll (in diesem Beispiel die Cisco IOS CA), und um Eigenschaften für die Vertrauenspunkt-CA anzugeben:

```
crypto ca trustpoint cisco
 enrollment retry count 5
 enrollment retry period 3
```

```
 enrollment url http://14.38.99.99:80
 revocation-check none
```

Hinweis: Der Befehl **crypto ca trustpoint** vereinheitlicht den vorhandenen **Crypto CA-Identitätsbefehl** und **verschlüsselt den Befehl "trust-root"**, wodurch eine kombinierte Funktionalität unter einem einzigen Befehl bereitgestellt wird.

3. Verwenden Sie den Befehl **crypto ca authentication cisco** (cisco ist die Trustpoint-Bezeichnung), um das Stammzertifikat vom CA-Server abzurufen:
```
R2(config)#crypto ca authenticate cisco
```

4. Verwenden Sie den Befehl **crypto ca enroll cisco** (cisco ist die Trustpoint-Bezeichnung), um sich anzumelden und Folgendes zu generieren:
```
R2(config)#crypto ca enroll cisco
```

Nachdem Sie sich erfolgreich beim Cisco IOS CA-Server angemeldet haben, sollten Sie die ausgestellten Zertifikate mit dem Befehl **show crypto ca certificate** sehen. Dies ist die Ausgabe des Befehls. Der Befehl zeigt detaillierte Zertifikatsinformationen an, die den im Cisco IOS CA-Server konfigurierten Parametern entsprechen:

```
R2#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 02
  Certificate Usage: General Purpose
  Issuer:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Subject:
    Name: R2.cisco.com
    hostname=R2.cisco.com
  CRL Distribution Point:
 http://172.18.108.26/cisco1cdp.cisco1.crl
Validity Date:
    start date: 15:41:11 UTC Jan 21 2004
    end   date: 15:41:11 UTC Aug 8 2004
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: cisco

CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Issuer:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Subject:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Validity Date:
    start date: 15:39:00 UTC Jan 21 2004
    end   date: 15:39:00 UTC Jan 20 2005
  Associated Trustpoints: cisco
```

5. Geben Sie den folgenden Befehl ein, um den Schlüssel im persistenten Flash-Speicher zu speichern:
```
hostname(config)#write memory
```

6. Geben Sie den folgenden Befehl ein, um die Konfiguration zu speichern:

```
hostname#copy run start
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show crypto ca certificate**: Zeigt Zertifikate an.
- **show crypto key mypubkey rsa**: Zeigt das Schlüsselpaar an.

```
!% Key pair was generated at: 09:28:16 EST Jan 30 2004
  !Key name: ese-ios-ca
  ! Usage: General Purpose Key
  ! Key is exportable.
  ! Key Data:
  !  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AF2198
  !  C56F1A8F 5AC501FF ADFB1489 1F503F91 CA3C3FA3 9FB2C150 FFCBF815 2AA73060
  !  E79AF510 E292C171 C6804B45 0CAAD4AF 5834AB85 B204208B 3960D20D 9B51AF7B
  !  ACF12D3D F5BC6EAE 77186AE9 1471F5A4 443CE5B5 1336EC33 5FEB3398 002C15EE
  !  9F8FD331 83490D8A 983FBBE1 9E72A130 121A3B97 A3ACD147 C37DA3D6 77020301 0001
  !% Key pair was generated at: 09:28:17 EST Jan 30 2004
  !Key name: ese-ios-ca.server
  ! Usage: Encryption Key
  ! Key is exportable.
  ! Key Data:
  !  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 0096456A 01AEC6A5
  !  0049CCA7 B41B675E 5317328D DF879CAE DB96A739 26F2A03E 09638A7A 99DFF8E9
  !  18F7635D 6FB6EE27 EF93B3DE 336C148A 6A7A91CB 6A5F7E1B E0084174 2C22B3E2
  !  3ABF260F 5C4498ED 20E76948 9BC2A360 1C799F8C 1B518DD8 D9020301 0001
```

- **crypto pki server ese-ios-ca info crl**: Zeigt die Zertifikatswiderrufliste (CRL) an.

```
! Certificate Revocation List:
  !    Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
  !    This Update: 09:58:27 EST Jan 30 2004
  !    Next Update: 09:58:27 EST Jan 31 2004
  !    Number of CRL entries: 0
  !    CRL size: 300 bytes
```

- **crypto pki server ese-ios-ca info request**: Zeigt ausstehende Registrierungsanfragen an.

```
! Enrollment Request Database:
  ! ReqID  State      Fingerprint                      SubjectName
  ! --------------------------------------------------------------------
```

- **show crypto pki server**: Zeigt den aktuellen Status des PKI-Servers (Public Key Infrastructure) an.

```
! Certificate Server status: enabled, configured
  !    Granting mode is: manual
  !    Last certificate issued serial number: 0x1
  !    CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
  !    CRL NextUpdate timer: 09:58:26 EST Jan 31 2004
  !    Current storage dir: nvram:
  !    Database Level: Names - subject name data written as .cnm
```

- **crypto pki server *cs-label* grant { all | *tranaction-id* }**: Gewährt alle oder spezifische SCEP-Anfragen.
- **crypto pki server *cs-label* reject { all | *tranaction-id* }**: Alle oder bestimmte SCEP-Anforderungen werden abgelehnt.

- **crypto pki server cs-label password generate [** ***minutes*** **]** - Generiert ein einmaliges Kennwort (OTP) für eine SCEP-Anforderung (Minuten - Dauer (in Minuten), die das Kennwort gültig ist. Der gültige Bereich liegt zwischen 1 und 1440 Minuten. Der Standardwert ist 60 Minuten.**Hinweis:** Es ist jeweils nur ein OTP gültig. Wenn ein zweites OTP generiert wird, ist das vorherige OTP nicht mehr gültig.
- **crypto pki server** ***cs-label*** **widerrufen** ***certificate-serial-number*** **- Ruft ein Zertifikat auf der Grundlage seiner Seriennummer auf.**
- **crypto pki server** ***cs-label*** **request** ***pkcs10*** **{url** ***url*** **|** ***terminal*****} [pem]**: Fügt der Anforderungsdatenbank manuell entweder die Base64- oder die PEM PKCS10-Zertifikatsanmeldungsanfrage hinzu.
- **crypto pki server** ***cs-label*** **info crl**: Zeigt Informationen zum Status des aktuellen CRL an.
- **crypto pki server** ***cs-label*** **info request** - Zeigt alle ausstehenden Zertifikatsanmeldungsanforderungen an.

Weitere Informationen zur Überprüfung finden Sie im Abschnitt Überprüfen des generierten Schlüsselpaars dieses Dokuments.

Fehlerbehebung

Informationen zur Fehlerbehebung finden Sie unter IP Security Troubleshooting - Understanding and Using debug Commands for Troubleshooting.

Hinweis: In vielen Situationen können Sie die Probleme beheben, wenn Sie den CA-Server löschen und neu definieren.

Zugehörige Informationen

- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems